PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G06K 17/00 — A1

(11) Internationale Veröffentlichungsnummer: WO 98/52150

(43) Internationales Veröffentlichungsdatum: 19. November 1998 (19.11.98)

(21) Internationales Aktenzeichen: PCT/DE98/01360

(22) Internationales Anmeldedatum: 15. Mai 1998 (15.05.98)

(30) Prioritätsdaten:
197 20 431.7 15. Mai 1997 (15.05.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: BETARESEARCH, GESELLSCHAFT FÜR ENTWICKLUNG UND VERMARKTUNG DIGITALER INFRASTRUKTUREN MBH [DE/DE]; Betastrasse 1, D–85774 Unterföhring (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HAGN, Thomas [DE/DE]; Dreifaltigkeitsplatz 12, D–84028 Landshut (DE).

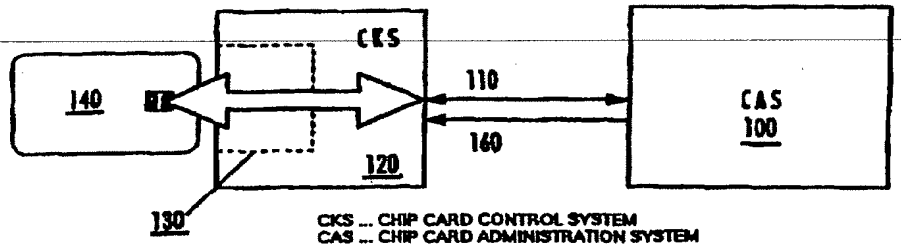
(74) Anwalt: BETTEN & RESCH; Reichenbachstrasse 19, D–80469 München (DE).

(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: DEVICE AND METHOD FOR PERSONALISING CHIP CARDS

(54) Bezeichnung: VORRICHTUNG UND VERFAHREN ZUR PERSONALISIERUNG VON CHIPKARTEN



(57) Abstract

The invention relates to a method for executing an electronic personalization and/or initialisation of a chip card, and/or a chip card application, characterised by the following steps: contacting the chip card using a first device; constructing or providing a connection between said first device and a separate second device for creating a logical communication channel to allow communication between the chip card and the second device via the first device; request from the first device to the second device to execute a personalization and/or initialisation of the chip card, and/or to execute a chip card application; and execution of the requested personalization and/or initialisation of the chip card, and/or the requested chip card application with transparent transmission of data and/or commands between the chip card and the second device via the logical communication channel.

(57) Zusammenfassung

Verfahren zum Durchführen einer elektronischen Personalisierung und/oder Initialisierung einer Chipkarte und/oder einer Chipkartenanwendung, gekennzeichnet durch die folgenden Verfahrensschritte : Kontaktieren der Chipkarte durch eine erste Vorrichtung; Aufbauen oder Bereitstellen einer Verbindung zwischen der ersten Vorrichtung und einer separaten zweiten Vorrichtung zur Ausbildung eines logischen Kommunikationskanals zur Ermöglichung einer Kommunikation zwischen Chipkarte und der zweiten Vorrichtung über die erste Vorrichtung; Anfordern der Durchführung einer Personalisierung und/oder Initialisierung der Chipkarte und/oder der Durchführung einer Chipkartenanwendung durch die zweite Vorrichtung von der ersten Vorrichtung; und Durchführung der angeforderten Personalisierung und/oder Initialisierung der Chipkarte und/oder der angeforderten Chipkartenanwendung unter Verwendung der transparenten Übertragung von Daten und/oder Befehlen zwischen Chipkarte und zweiter Vorrichtung über den logischen Kommunikationskanal.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

Vorrichtung und Verfahren zur Personalisierung von Chipkarten

Die vorliegende Erfindung betrifft eine Vorrichtung und ein Verfahren zur Personalisierung von Chipkarten.

Chipkarten werden in vielen Systemen mit hohen Sicherheitsanforderungen eingesetzt, um systeminterne Schlüssel den Kunden des Systems vor Ort bereitzustellen, ohne daß ein direkter Zugriff auf diese Schlüssel unter Umgehung des Systems möglich ist. Chipkarten werden als Sicherheits- bzw. Berechtigungsausweis eingesetzt und ermöglichen, über die auf ihnen gespeicherten Schlüssel und Algorithmen, eine sichere Authentifizierung und eine Verschlüsselung von Datenströmen. Auf Daten, die in Chipkarten während der Initialisierung und Personalisierung abgelegt werden, können nur authorisierte Systeme nach einer entsprechenden Authentifizierung zugreifen, bei der die Berechtigung überprüft wird.

Anwendungsbeispiele für Systeme mit Chipkarten sind z.B. Mobilfunksysteme, Banksysteme mit Bankkarten oder Pay-TV Systeme.

Bei der Initialisierung und Personalisierung von Chipkarten werden die für den späteren Einsatz notwendigen Daten in den Chip der Chipkarte programmiert. Diese in gewisser Weise noch zum Produktionsvorgang gehörenden Bearbeitungsphasen im Chipkarten-Lebenszyklus stellen in diesem Zusammenhang Prozesse dar, an die höchste Sicherheitsanforderungen gestellt werden müssen. So werden beispielsweise bei der Initialisierung und Personalisierung Schlüssel auf die Karte gebracht, die im späteren Einsatz der Karte benötigt werden, die aber auch, wenn sie ausspioniert werden, die Sicherheit des gesamten Anwendungssystems der Chipkarten gefährden könnten.

Bei der Initialisierung wird eine Chipkarte beispielsweise "programmiert", das heißt es werden Daten in die Chipkarte geschrieben, die sie in die Lage versetzen, die ihr zugedachte Funktion zu erfüllen. Bei der Personalisierung ist mindestens ein Teil der auf die Chipkarte aufgebrachten Daten einzigartig, das heißt für jede einzelne

Chipkarte unterschiedlich, wodurch die Chipkarte individualisiert oder "personalisiert" wird. Die bei derartigen Vorgängen übertragenen Daten enthalten naturgemäß auch sicherheitsrelevante Daten wie etwa Schlüssel, aber auch die Abfolge von Befehlen sowie deren Struktur und Inhalt zur Durchführung einer Personalisierung oder Initialisierung selbst stellen bereits sicherheitskritische Informationen dar, die möglichst wenigen Personen zugänglich sein sollten.

In den herkömmlichen Systemen im Bereich der Chipkartenpersonalisierung ist die Komponente zur Durchführung der Ablauflogik, d. h. der Befehlsfolge der Chipkartenpersonalisierung, ein integraler Bestandteil des Systems, das auch das Kartenhandling und die Kartenkontaktierung durchführt. Kartenhandling heißt dabei das Zugänglichmachen der Chipkarte für Befehle und Daten von außen, also die Durchführung der elementar notwendigen physikalischen, hard- und softwäremäßigen Grundfunktionen, etwa das Kontaktieren der Karte und Versorgen der Karte mit der erforderlichen Betriebsspannung, aber auch etwa das Auslösen eines Reset der Karte, um so die Karte zur Durchführung einer Kommunikation mit der Außenwelt erst in die Lage zu versetzen.

Dies bedeutet, daß die Logik, die der Chipkartenpersonalisierung zugrunde liegt, die Algorithmen und Schlüssel dazu, in diesem System verankert sind und somit dem Lieferanten dieses Systemes bekannt gemacht werden bzw. im System abgelegt werden müssen. Diese Situation führt dazu, daß den Herstellern von Personalisierungssystemen sicherheitsrelevante Informationen über die Logik der Chipkartenpersonalisierung, Teile der Chipkarten-Kommandoschnittstelle, sowie über Algorithmen und Schlüssel gegeben werden müssen. Das Verteilen von Informationen mit einem so hohen Sicherheitsgrad stellt ein erhöhtes Sicherheitrisiko dar. Kenntnisse über die Logik der Chipkarten erleichtern Angriffe auf die Sicherheitsmechanismen des Chips auf der Karte. Sicherheitslöcher, die absichtlich oder unabsichtlich vom Hersteller in die Systeme gebracht wurden, könnten zur Kompromittierung der Chipkarten und zum Ausspähen von Schlüsseln führen und somit das Anwendungssystem der Chipkarte gefährden.

Es ist daher eine Aufgabe der vorliegenden Erfindung, eine Vorrichtung und ein Verfahren zur Chipkartenpersonalisierung zu schaffen, das eine erhöhte Sicherheit aufweist.

Eine weitere Aufgabe der vorliegenden Erfindung besteht in der Trennung der Sicherheitslogik (z.B. Befehlsofolge der Personalisierung, Authentifizierung, usw.) und des Kartenhandlings. Dabei sollte aber der Kommunikationsweg und die Anforderung der Anwendung von dem System vorgegeben werden, das die Chipkarten kontaktiert.

Ein wesentlicher Aspekt der vorliegenden Erfindung besteht darin, daß zum Durchführen von Personalisierung, Initialisierung oder sicherheitskritischen Chipkartenanwendungen ein separates Sicherheitssystem vorgesehen ist. Dabei werden elektronische administrative Bearbeitungsschritte (Personalisierung, Initialisierung) und sicherheitskritische Anwendungen mit Chipkarten (Authentifizierung) innerhalb der Chipkartenlebensdauer vom System zum Kartenhandling bzw. zur Chipkontaktierung getrennt.

Die Ablauflogik der elektronischen Personalisierung und Initialisierung von Chipkarten, die Chipkarten-Kommandoschnittstelle, d. h. die Softwareschnittstelle, die den der Chipkarte zur Verfügung stehenden Befehlssatz darstellt, ferner Algorithmen und die notwendigen Schlüssel zum Personalisieren werden in einem zentralen Sicherheitssystem implementiert, das nach einer Anforderung von einem sogenannten Chipkarten-Kontrollsystem, das das Kartenhandling und -kontaktieren durchführt, diese Aufgaben durchführen kann.

Das System zum Kartenhandling und -kontaktieren sorgt dafür, daß ein sogenannter logischer Kommunikationskanal zwischen dem Chip der Karte und dem Sicherheitssystem zur elektronischen Personalisierung und Initialisierung aufgebaut wird.

Unter einem Kommunikationskanal ist dabei eine Verbindung zwischen zwei an der Kommunikation beteiligten Partnern zu verstehen, über die Daten ausgetauscht

werden können. Die Verbindung muß nicht unbedingt direkt zwischen den beiden Partnern bestehen, sondern kann über eine oder mehrere Zwischenstationen erfolgen, so daß dann anstelle einer tatsächlichen direkten Verbindung eine indirekte oder "logische Verbindung" zwischen den Partnern besteht. Die Kommunikationsendpunkte sind in einem solchen Fall nicht direkt miteinander verbunden, sondern entlang eines Datenpfades, der eine Verknüpfung oder Verbindung zwischen den beiden Kommunikationsendpunkten herstellt und einen Datenweg oder "logischen Kommunikationskanal" zur Verfügung stellt, über den der Datenaustausch zwischen den Kommunikationsendpunkten unabhängig von dem tatsächlichen hardwaremäßigen Verbindungsweg zwischen den beiden Kommunikationsendpunkten - ob direkt oder über eine Zwischenstation - in korrekter Weise erfolgen kann. Der zu verwendende logische Kommunikationskanal wird dem zentralen Sicherheitssystem in einer Anforderung zur Durchführung einer Chipkartenpersonalisierung oder einer anderen Chipkartenanwendung mitgeteilt.

Das zentrale System zum Durchführen der Personalisierung, Initialisierung, Konfigurierung einer Chipkarte, oder zur Durchführung einer Chipkartenanwendung ermöglicht in einem bevorzugten Ausführungsbeispiel die Anbindung an verschiedene Kartenhandlingsysteme bzw. sogenannte Chipkarten-Kontrollsysteme. Das System erhält eine Anforderung eines Chipkarten-Kontrollsystems zum Durchführen einer Chipkartenpersonalisierung, -initialisierung oder -anwendung und führt im Anschluß daran die angeforderte Ablauflogik (z.B. Personalisieren einer Chipkarte), das heißt die entsprechende Abfolge von Befehlen und Daten über einen logischen Kommunikationskanal durch, der einen Datenpfad zwischen dem zentralen System und der Chipkarte darstellt.

In der Anforderung an das zentrale System zur Personalisierung, Initialisierung, Konfigurierung einer Chipkarte oder zum Durchführen einer Chipkartenanwendung werden die für die Durchführung der angeforderten Anwendung bzw. der ihr entsprechenden Ablauflogik, d. h. der ihr entsprechenden Folge von Befehlen, notwendigen Informationen übertragen, beispielsweise Informationen über das zu verwendende Kommunikationsprotokoll. Wenn nachfolgend der Einfachheit halber lediglich von einer angeforderten Anwendung die Rede ist, so sei damit auch die

Möglichkeit eingeschlossen, daß es sich bei der angeforderten Anwendung neben weiteren Chpikartenanwendungen insbesondere auch um eine Personalisierung oder um eine Initialisierung einer Chipkarte handeln kann.

Die Kommunikation der Kommandos und Nachrichten (Messages) zu und von der Chipkarte verläuft transparent, das heißt die übertragenen Daten werden unverändert zwischen den beteiligten Kommunikationspartnern übertragen, beziehungsweise die von einem Endpunkt der Kommunikation (Chipkarte oder zentrales System) zum anderen Endpunkt (zentrales System oder Chipkarte) abgesandten Daten erreichen ihren Bestimmungsort in unveränderter Form. Ein solcher transparenter Kommunikationskanal wird vom System zum Kartenhandling und Kartenkontaktieren, dem Kontrollsystem, bereitgestellt oder aufgebaut. Der Kommunikationsweg, also der Eintrittspunkt des logischen Kommunikationskanals in das Chipkarten-Kontrollsystem, über den die Kommunikation stattfinden soll, und das Kommunikationsprotokoll werden bei der Anforderung der Anwendung dem zentralen Sicherheitssystem mitgeteilt.

Nachfolgend wird die vorliegende Erfindung anhand mehrerer Ausführungsbeispiele unter Bezugnahme auf die beiliegenden Zeichnungen im Detail beschrieben. Dabei zeigen:

Fig. 1 eine schematische Darstellung des Gesamtkonzepts gemäß einem ersten Ausführungsbeispiel der vorliegenden Erfindung;
Fig. 2 eine schematische Darstellung der Verfahrensschritte gemäß dem ersten Ausführungsbeispiel der vorliegenden Erfindung;
Fig. 3 eine schematische Darstellung der Elemente des Gesamtkonzepts gemäß einem zweiten Ausführungsbeispiel der vorliegenden Erfindung.

Nachfolgend werden die Elemente eines ersten Ausführungsbeispiels der Erfindung unter Bezugnahme auf Figur 1 näher erläutert.

Ein Chipkarten-Administrationssystem (CAS) 100 gemäß Figur 1 ist ein System zur Personalisierung, Initialisierung bzw. zur Durchführung von sicherheitskritischen

Anwendungen mit Chipkarten (z.B. Authentifizierung). Es ist über einen Kommunikationskanal 110, d. h. über eine Verbindung entlang derer Daten ausgetauscht werden können, mit einem Chipkartenkontrollsystem (CKS) 120 verbunden. Ein Chipkarten-Koppler 130 ist Bestandteil des Kontrollsystems 120 und ist für die physikalische Kontaktierung einer Chipkarte 140 verantwortlich.

Ein Chipkarten-Koppler 130 wird hier als integraler Bestandteil des Chipkarten-Kontrollsystems betrachtet. Er führt die Kommunikation mit der Chipkarte auf der physikalischen Ebene durch und veranlaßt den Chipkarten-Reset durch das entsprechende elektronische Signal. Üblicherweise stellt der Chipkarten-Koppler dem Chipkarten-Kontrollsystem CKS eine Kommandoschnittstelle, das heißt einen bestimmten Satz von Befehlen zur Verfügung, die er dann jeweils in die entsprechende für die Chipkarte verständliche elektronische Signalfolge umwandelt. Auf der Basis dieser Kommandoschnittstelle kommuniziert das Chipkarten-Kontrollsystem mit der Chipkarte.

Ein dadurch realisierter Kommunikationskanal 150 stellt eine Verbindung zwischen der Chipkarte 140 und dem Chipkarten-Kontrollsystem CKS 120 her. Der Kommunikationskanal 150 und der Kommunikationskanal 110 bilden zusammen einen logischen Kommunikationskanal, der den Datenaustausch zwischen der Chipkarte 140 und dem Chipkartenadministrationssystem 100 ermöglicht.

Der Datenaustausch zwischen dem CKS und dem CAS über den Kommunikationskanal 110 erfolgt dabei nach einem bestimmten Protokoll. Gemäß diesem Protokoll werden etwa die vom CAS an das CKS zu übertragenden Daten "gepackt", d. h. formatiert, und die vom CKS empfangenen Daten werden "entpackt", d. h. die entsprechenden Nutzdaten, beispielsweise Befehle für die Chipkarte, werden in dem eintreffenden Datenstrom identifiziert und diese werden dann wiederum über den Kommunikationskanal 150 an die Chipkarte 140 weitergeleitet.

Über einen weiteren zur Steuerung dienenden Kommunikationskanal 160 können Befehle und Nachrichten zwischen dem Kontrollsystem 120 und dem Chipkarten-Administrationssystem 100 ausgetauscht werden, wodurch dem Chipkarten-

Administrationssystem eine steuernde Einflußnahme auf das Kontrollsystem ermöglicht wird.

Dabei können die beiden Kommunikationskanäle 160 durchaus über die hardwaremäßig gleiche Verbindung realisiert werden. Dies geschieht beispielsweise, indem das Kommunikationsprotokoll beziehungsweise die Steuerdaten oder Header der übertragenen Daten eine Identifikation des Bestimmungsortes vorsehen und somit den Kommunikationskanal bezüglich seines Start- und Zielpunktes identifizieren und definieren. Das CKS ist dann beispielsweise in der Lage, die über eine einzige hardwaremäßige Leitung eintreffenden Daten bezüglich ihres Zielortes, etwa Chipkarte oder CKS selbst, zu identifizieren und entsprechend weiterzuleiten oder selbst zu verarbeiten.

Das Chipkarten-Administrationssystem führt seine Aufgaben auf Anforderung von dem Chipkarten-Kontrollsystem CKS hin durch. Dem Chipkarten-Administrationssystem CAS werden dazu vom Chipkarten-Kontrollsystem die beiden Kommunikationskanäle 110 und 160, beziehungsweise die CKS-seitigen Kommunikationsendpunkte zur Ausbildung der Kommunikationskanäle zur Verfügung gestellt, die zum einen die Kommunikation mit der Chipkarte 140 über den weiteren Kommunikationskanal 150, zum anderen die Kommunikation mit dem Kontrollsystem 120 ermöglichen.

Das Chipkarten-Administrationssystem CAS hat alle Schlüssel und Algorithmen, die notwendig sind, um die notwendige Anwendungslogik für die Initialisierung, Personalisierung oder die sicherheitsrelevanten Anwendungen wie etwa eine Authentifizierung mit der Karte durchzuführen. Erst nachdem das Chipkarten-Kontrollsystem 120 den Chip der Karte kontaktiert und einen Kommunikationskanal zum Chip eingerichtet hat, kann das Chipkarten-Administrationssystem CAS seine Aufgaben durchführen.

Das Chipkarten-Kontrollsystem ist ein System, das eine Kontaktierung des Chips der Karte herstellt und somit eine Kommunikation mit dem Chip ermöglicht. Dies geschieht, indem zunächst der physikalische Kontakt zum Chip der Karte hergestellt

wird. Daraufhin wird gemäß ISO 7816 ein Reset der Chipkarte durchgeführt, das heißt die Chipkarte wird durch Anlegen eines bestimmten Signals, des sogenannten Reset-Signals, veranlaßt, mit einer Antwortnachricht, dem sogenannten "Answer to Reset ATR" zu antworten. Diese Antwortnachricht enthält beispielsweise Daten, die die Chipkarte bezüglich des zu verwendenden Kommunikationsprotokolls, der Taktfrequenz, etc., identifizieren. Das Chipkarten-Kontrollsystem CKS stellt dann den ersten Kommunikationskanal 110, bzw. den entsprechenden CKS-seitigen Kommunikationsendpunkt, für das Chipkarten-Administrationssystem CAS 100 bereit und baut so zusammen mit dem CAS den logischen Kommunikationskanal zwischen Chipkarte und Chipkarten-Administrationssystem entlang der Kommunikationskanäle 110 und 150 auf. Ein zweiter Kommunikationskanal 160 zwischen Chipkarten-Kontrollsystem CKS und Chipkarten-Administrationssystem CAS wird zur Abstimmung und Kontrolle zwischen beiden Systemen vom Chipkarten-Kontrollsystem zur Verfügung gestellt.

Der logische Kommunikationskanal zwischen Chipkarte und Chipkarten-Administrationssystem CAS, bestehend aus den beiden Kommunikationskanälen 110 und 150, ist ein transparenter Kommunikationskanal, das heißt die Kommunikation zwischen CAS und Chipkarte erfolgt transparent. Transparente Kommunikation heißt dabei, daß die jeweils vom CAS abgeschickten Befehle oder Daten, die direkt für die Chipkarte bestimmt sind, unverändert an die Chipkarte übertragen werden. Umgekehrt werden Nachrichten, die von der Chipkarte stammen und für das CAS bestimmt sind, unverändert über den transparenten logischen Kommunikationskanal an das CAS übertragen. Handelt es sich also bei den ausgetauschten Informationseinheiten um sogenannte Datentelegramme, die einen Steuerteil und einen Datenteil umfassen, so werden die direkt für einen Kommunikationszielpunkt, also Chipkarte oder CAS, bestimmten Teile dieser Datentelegrammme unverändert an den entsprechenden Kommunikationszielpunkt übertragen. Das Chipkarten-Kontrollsystem stellt also einen transparenten logischen Kommunikationskanal als eine Verbindung zwischen Chipkarte und Chipkarten-Administrationssystem zur Verfügung.

Gemäß dem ersten Ausführungsbeispiel der Erfindung tritt das System zum Handling von Chipkarten bzw. zum Kontaktieren von Chips, das Chipkarten-Kontrollsystem CKS, zwecks Durchführen einer elektronischen Personalisierung bzw. Initialisierung von Chipkarten oder zur Durchführung einer Chipkartenapplikation mit dem Chipkarten-Administrationssystem CAS als einem separaten Sicherheitssystem in Verbindung und fordert die Ausführung einer dieser Anwendungen für eine Chipkarte über den Kommunikationskanal 160 an. Als Anwendungen kommen hier elektronische administrative Bearbeitungsschritte an Chipkarten (Personalisierung, Initialisierung) oder sicherheitskritische Anwendungen mit Chipkarten (z.B. Authentifizierung) innerhalb des Lebenszyklus einer Chipkarte in Frage. Für den Fall einer Personalisierung werden dabei beispielsweise spezielle Schlüssel für jede Chipkarte und/oder Algorithmen bzw. sonstige Daten auf die Chipkarte aufgebracht, die die Chipkarte dann als eine ganz spezielle Chipkarte mit entsprechender Funktion ausweisen und sie so als die spezielle Chipkarte ihres jeweiligen Benutzers kenntlichmachen oder personalisieren.

Nach Anforderung der Anwendung durch das Chipkarten-Kontrollsystem CKS führt das Chipkarten-Administrationssystem CAS eine Ablauflogik für die angeforderte Anwendung aus. Die Ablauflogik besteht dabei aus einer Folge von Befehlen und Daten an die Chipkarte sowie den zugehörigen Antwortnachrichten, die in ihrer Summe die angeforderte Anwendung darstellen. Im Verlauf der Anwendung werden über den beschriebenen transparenten logischen Kommunikationskanal die Befehle und Daten transparent an die Chipkarte gesandt und umgekehrt, über den gleichen logischen Kommunikationskanal, resultierende Meldungen oder Antwortnachrichten von der Chipkarte vom Chipkarten-Administrationssystem CAS empfangen. Dieser logische Kommunikationskanal stellt somit eine transparente Verbindung zwischen Chipkarte und Chipkarten-Administrationssystem CAS her. Das Chipkarten-Kontrollsystem CKS baut diese Verbindung auf und gewährleistet die transparente Übertragung von Datentelegrammen von und zur Chipkarte.

Informationen über den zu verwendenden Kommunikationkanal werden in der Anforderung der Anwendung durch das Chipkarten-Kontrollsystem CKS an das Chipkarten-Administrationssystem übermittelt. Die über die Anforderung

übertragenen Informationen enthalten u.a. die Kommunikationsadresse, d. h. die Identifizierung des zuverwendenden Eintrittspunkts des Kommunikationskanals in das CKS, sowie ferner das Kommunikationsprotokoll, die für den bereitgestellten Kommunikationskanal verwendet werden müssen, und Informationen über die Anwendung, die durchzuführen ist. Beginnt eine Chipkartenanwendung mit einem Reset der Chipkarte nach ISO 7816 wird dieser Chipkartenreset vor der Anwendungsanforderung vom Chipkarten-Kontrollsystem durchgeführt und die Ergebnisse des Resets (Answer to Reset) werden ebenfalls in der Anwendungsanforderung an das Chipkarten-Administrationssystem übertragen.

Auch während der Ausführung der Ablauflogik der angeforderten Anwendung kann unter Umständen das Chipkarten-Kontrollsystem vom Chipkarten-Administrationssystem zu einem Reset der Karte aufgefordert werden, etwa falls dies als ein Teil der Ablauflogik vorgesehen ist. Dies kann aber beispielsweise auch geschehen, wenn bei der Durchführung der Anwendung ein Fehler aufgetreten ist. Der Reset wird dann vom CAS angefordert und die resultierenden Reset-Informationen werden dann nach dem Reset dem Chipkarten-Administrationssystem mitgeteilt. Daraufhin kann erneut die zur Durchführung der Anwendung erforderliche Ablauflogik unter Verwendung der transparenten Kommunikation durchgeführt werden oder, falls der Reset Teil der Ablauflogik ist, sie an der entsprechenden Stelle fortgesetzt werden.

Nach Beendigung der Ablauflogik teilt das Chipkarten-Administrationssystem dem Chipkarten-Kontrollsystem das Ende der Anwendung zusammen mit einem Ergebnis oder einer Resultatnachricht bezüglich der Anwendung mit. Dieses Ergebnis kann beispielsweise in der Meldung bestehen, daß die Anwendung erfolgreich durchgeführt wurde, es sind jedoch auch noch weitere Formen und Inhalte der Resultatnachricht denkbar. So kann die Resultatnachricht auch weitere Informationen bezüglich der durchgeführten Anwendung enthalten. Bei erfolgreicher Durchführung der Anwendung kann der zur Durchführung der Anwendung aufgebaute transparente logische Kommunikationskanal nun wieder abgebaut werden und die Chipkarte kann dekontaktiert werden. wurde die Anwendung nicht

erfolgreich durchgeführt kann aber auch beispielsweise ein neuer Versuch gestartet werden.

Die einzelnen Teilschritte die gemäß dem ersten Ausführungsbeispiel der Erfindung durchgeführt werden, sind nachfolgend noch einmal summarisch aufgelistet:

1) Chipkarten-Reset, ausgelöst durch das Chipkarten-Kontrollsystem CKS bzw. dem Chipkarten-Koppler nach erfolgter Chipkontaktierung.
2) Aufbauen eines logischen Kommunikationskanals für eine transparente Kommunikation zwischen Chipkarte und Chipkarten-Administrationssystem durch das Chipkarten-Kontrollsystem.
3) Anforderung einer Anwendung, übermittelt an das Chipkarten-Administrationssystem, mit Informationen über den zu verwendenden Kommunikationskanal, über den Chip-Reset aus Schritt 1 ("answer to reset"-Informationen) und über die Anwendung, die durchzuführen ist.
4) Transparente Kommunikation zwischen Chipkarten-Administrationssystem und Chipkarte zur direkten Übermittlung von Kartenkommandos und Antwortnachrichten während der Durchführung der Ablauflogik der Anwendung. Die transparente Kommunikation wird dabei durch das Chipkarten-Kontrollsystem gewährleistet.
5) Falls erforderlich (z.B. bei Personalisierung), Anforderung eines Chip-Resets vom Chipkarten-Administrationssystems und der Resetinformation durch das Chipkarten-Kontrollsystem.
6) Mitteilen eines Ergebnisses bezüglich der Anwendung an das Chipkarten-Kontrollsystem durch das Chipkarten-Administrationssystem.
7) Eventuell Abbau des logischen Kommunikationsweges durch das Chipkarten-Kontrollsystem .

Der Ablauf ist für den Fall einer Chipkartenpersonalisierung gemäß dem ersten Ausführungsbeispiel in Figur 2 schematisch dargestellt. Dabei stellt die linke Seite das CAS dar, in dem die Personalisierung durchführt wird. Über den mittleren Teil, das CKS, werden Kommandos und Antwortnachrichten (Responses) über den Koppler CC transparent an die Chipkarte übertragen.

Folgende Grundprinzipien liegen dem beschriebenen Konzept zugrunde:

- transparenter logischer Kommunikationskanal:
  Das Chipkarten-Kontrollsystem ermöglicht eine transparente Kommunikation zwischen Chipkarte und Chipkarten-Administrationssystem durch Bereitstellung eines transparenten logischen Kommunikationskanals.

- Anforderung der Anwendung:
  Eine Anforderung zum Durchführen einer Anwendung wird vom Chipkarten-Kontrollsystem an das Chipkarten-Administrationssystem CAS gesandt. Die Anforderung enthält Informationen über die auszuführende Anwendung und den dafür zu verwendenden transparenten logischen Kommunikationskanal sowie das Kommunikationsprotokoll. Es werden also mit der Anforderung folgende Informationen übertragen:
  - Informationen bezüglich der Kommunikation (Adresse des zur Verfügung gestellten Kommunikationskanals, des zu verwendenden Protokolls)
  - Identifikation der angeforderten Anwendung
  - Informationen bezüglich der kontaktierten Chipkarte aus den Resetinformationen (answer to reset)
  - gegebenenfalls eine Identifikationskennung der Anwendungsanforderungen der Chipkarte innerhalb des Chipkarten-Kontrollsystems zur Ermöglichung der Re-Identifizierung der Anwendungsanforderungen,

-Rückmeldung des Anwendungsergebnisses:
  Das Chipkarten-Administrationssystem meldet ein Ergebnis bezüglich der Anwendungsdurchführung an das Chipkarten-Kontrollsystem zurück. Die Rückmeldung enthält dabei folgende Informationen:
  - Ergebnis bezüglich der Anwendung, die sogenannte Resultatnachricht
  -gegebenenfalls eine Identifikation der Anwendungsanforderungen der Chipkarte innerhalb des Chipkarten-Kontrollsystem

Der Personalisierungsprozeß wird nach dem oben beschriebenen Konzept von zwei getrennten Systemen, dem Chipkarten-Kontrollsystem CKS und dem Chipkarten-Administrationssystem CAS durchgeführt. Das Chipkarten-Kontrollsystem übernimmt dabei das Handling bzw. das Kontaktieren der Chipkarte und führt die Kommunikation über den Chipkarten-Koppler auf der physikalischen Ebene durch. Im Chipkarten-Kontrollsystem müssen keine Informationen über Ablauflogik, Chipkarten-Kommandoschnittstelle, Schlüssel und Algorithmen der elektronischen administrativen Chipkartenbearbeitung und der Chipkartenapplikationen gespeichert werden. Das Chipkarten-Kontrollsystem sorgt dafür, daß eine elektrische Verbindung mit dem Chip auf der Karte hergestellt wird, und dient als Router, das heißt als Zwischenstation, für die transparente Kommunikation mit der Chipkarte. Das Chipkarten-Kontrollsystem bestimmt als auslösendes bzw. anforderndes System die Art der Anwendung die vom Chipkarten-Administrationssystem durchgeführt werden soll.

Die Durchführung der Anwendung dagegen findet im Chipkarten-Administrationssystem statt. Ablauflogik, Algorithmen für die Anwendung mit der Chipkarte und entsprechende Schlüssel können hier in einem separaten System gespeichert und gut abgesichert werden. Spezifische Kenntnis über die Ablauflogik in der Chipkarte, die Chipkarten-Komandoschnittstelle und die Algorithmen werden somit nur zur Entwicklung des Chipkarten-Administrationssystems benötigt.

Die Kommunikation zwischen Chipkarten-Kontrollsystem und Chipkarten-Administrationssystem kann über ein Standardnetzwerk durchgeführt werden. Über den Anforderungsmechanismus können das Protokoll und der logische Kommunikationskanal, der für die Anwendung zu verwenden ist, in der Anforderung definiert werden.

Es können über ein zentrales Chipkarten-Administrationssystem verschiedene Anwendungen, wie Personalisierung, Initialisierung, Chipkarten-Authentifizierung, gleichzeitig betrieben werden. Alle dafür notwendigen sicherheitsrelevanten Daten und Algorithmen müssen dazu nur in einem zentralem Sicherheitssystem implementiert und verwaltet werden.

Über den Mechanismus der Anwendungsanforderung an das Chipkarten-Administrationssystem können die verschiedenen Anwendungen von verschiedenen Partnersystemen bzw. Chipkarten-Kontrollsystemen angefordert werden. Welche Kommunikationsmechanismen dabei verwendet werden sollen, wird jeweils bei der Anwendungsanforderung dem Chipkarten-Administrationssystem übermittelt.

So kann z.B. ein Point-of-Sales (POS)-Kartenleser, der über eine WAN-Verbindung zu erreichen ist, eine Rekonfiguration einer Chipkarte anfordern, während parallel ein Personalisierungssystem mit hohem Produktionsdurchsatz eine Personalisierungssequenz vom Chipkarten-Administrationssystem über eine LAN-Kommunikation anfordert.

Nachfolgend wird noch das Anwendungsbeispiel einer "Point of Sales (POS)"-Personalisierung beschrieben, also beispielsweise an einem dem Kunden zugänglichen Terminal.

Nachdem eine Kundenchipkarte in einem Chipkarten-Kontrollsystem kontaktiert wurde, wird eine Anfrage zur Personalisierung über ein WAN-Netzwerk an ein zentrales Chipkarten-Administrationssystem gesendet. Das Chipkarten-Administrationssystem verwendet den in der Anwendungsanforderung übertragenen Kommunikationskanal zur Chipkarten-Personalisierung. Ein Authentifizierung der Chipkarte mit dem Chipkarten-Administrationssystem wird durch eine gegenseitige Authentifizierung oder "mutual authentication" erreicht. Als zusätzlichen Sicherheitsmechanismus für die Aktion über das WAN/LAN-Netzwerk kann eine zusätzliche Verschlüsselung bei der Kommunikation überlagert werden. Informationen bezüglich der Methode der Verschlüsselung und Indizes auf die zu verwendenden Schlüssel können bei der Personalisierungsanforderung an das Chipkarten-Administrationssystem durch das Chipkarten-Kontrollsystem übertragen werden.

Ein typischer Anwendungsfall könnte eine Rekonfigurierung der Chipkarte entsprechend bestimmter am Point of Sales, also etwa an einem Terminal, vom Kunden definierter Anforderungen sein.

Nachfolgend wird unter Bezugnahme auf Fig. 3 ein zweites Ausführungsbeispiel der vorliegenden Erfindung beschrieben.

In diesem Ausführungsbeispiel werden mehrere Chipkarten 340 und 342 von einer Transporteinheit 322, die einen Teil des Chipkarten-Kontrollsystems 320 darstellt, transportiert und von einer Chipkarten-Kopplereinheit 324, die ebenfalls einen Teil des Chipkarten-Kontrollsystems 320 darstellt, kontaktiert. Die Kopplereinheit umfaßt dabei mehrere einzelne Koppler CC1 bis CC4, die jeweils eine Chipkarte kontaktieren können.

Ein Chipkarten-Administrationssystem (CAS) 300 ist auch im vorliegenden Beispiel ein Personalisierungssystem, das den Personalisierungsprozeß der Chipkarten durchführt. Nach dem Kontaktieren der Chipkarten wird es von dem Chipkarten-Kontrollsystem aufgerufen, und das Chipkarten-Administrationssystem CAS erzeugt die Personalisierungskommandos, leitet sie weiter und empfängt und verarbeitet die Antwortnachrichten von der Chipkarte. Das CAS ist auch hier kein Teil des Chipkarten-Kontrollsystems, sondern eine separate Vorrichtung, die mit dem Chipkarten-Kontrollsystem kommuniziert. Das Chipkarten-Kontrollsystem ist nicht mit der Erzeugung oder der Verschlüsselung von Chipkarten-Personalisierungskommandos und -nachrichten betraut.

Anstelle einer Personalisierung kann jedoch auch eine andere Anwendung vom CAS analog durchgeführt werden, beispielsweise eine Programmierung oder Verschlüsselung der Chipkarten. Auch in diesem Fall werden die entsprechenden Befehle vom CAS erzeugt und an die Chipkarte transparent übertragen.

Das Chipkarten-Kontrollsystem dient im Wesentlichen zum Weiterleiten von Nachrichten, um die Personalisierungsnachrichten zwischen der Chipkarte und dem Chipkarten-Administrationssystem weiterzuleiten. Die Antwortnachrichten der

Chipkarte sind gemäß dem definierten Kommunikationsprotokoll gepackt und werden über den entsprechenden Kommunikationskanal an das CAS weitergeleitet. Darüber hinaus ist das Chipkarten-Kontrollsystem als Steuerungseinheit mit dem Transport und dem Kontaktiermechanismus für die Chipkarten betraut. Hierfür ist im CKS eine Steuereinheit 326 vorgesehen.

Die Steuereinheit 326 steuert die Transporteinheit dabei beispielsweise so, daß neue Chipkarten, die personalisiert werden sollen, durch die Transporteinheit einem der Chipkarten-Koppler CC1 bis CC4 zugeführt und von diesem kontaktiert werden. Nach erfolgreicher Personalisierung werden die Chipkarten dann weitertransportiert und im Falle nicht erfolgreicher Personalisierung aussortiert. So können dann Chipkarten in großer Stückzahl personalisiert werden.

Das CKS löst durch eine entsprechende Anforderung die Personalisierungsverarbeitung aus, nachdem die Chipkarte physikalisch kontaktiert wurde. Das CKS, bzw. die Steuereinheit 326 des CKS, veranlaßt ferner über schematisch dargestellte Koppler-Kommunikationskanäle 330 und 332, die Verbindungen zwischen der Steuereinheit und den Chipkarten-Kopplern darstellen, die Auslösung des Reset durch die Koppler CC1 und CC3. Sie erhält daraufhin die "Answer-to-Reset"-Informationen, die von der Chipkarte ausgegeben werden, und überträgt diese mit einer Personalisierungsanforderung an das Chipkarten-Administrationssystem.

Nachfolgend wird unter Bezugnahme auf Figur 3 die Arbeitsweise der Kommunikationskanäle genauer beschrieben. Beim vorliegenden Ausführungsbeispiel sind mehrere Chipkarten-Koppler CC1 bis CC4 in das CKS integriert. Für jeden dieser Chipkarten-Koppler CC1 bis CC4 stellt das CKS einen Kommunikationskanal, bzw. einen entsprechenden CKS-seitigen Kommunikationsendpunkt 370 bis 376 zur Verfügung, der die Übertragung von Daten zwischen dem CAS und der Chipkarte ermöglicht. In Figur 3 sind die beiden Kommunikationskanäle 310 und 312 realisiert. Alle Personalisierungskommandos werden unter Verwendung dieser Kanäle an die entsprechenden Chipkarten-Koppler

und dann weiter an die Chipkarte geleitet, bzw. werden umgekehrt die Chipkartenantworten auf die Kommandos an das CAS gesandt.

So wird beispielsweise über den Kommunikationskanal 310 eine Verbindung vom CAS zum CKS-seitigen Kommunikationsendpunkt 370 hergestellt, von dort geht die Verbindung weiter über den Koppler CC1 zu der Chipkarte 340 und bildet so einen logischen Kommunikationskanal zwischen CAS und der Chipkarte 340. Im Fall der Chipkarte 342 läuft die Verbindung analog über den Kommunikationskanal 312.

Beim vorliegenden Ausführungsbeispiel verläuft die Kommunikation zwischen dem CKS und dem CAS unter Verwendung einer TCP/IP-Socketverbindung. Ein Socket ist ein Kommunikationsendpunkt. Das CKS liefert dabei Serversockets 370 bis 380 und das CAS stellt als Client unter Verwendung von Client-Sockets 390 die Verbindung zu diesen Server-Sockets her. Die vom CKS zur Verfügung gestellten Sockets lassen sich logisch in zwei Gruppen klassifizieren. Jede der Gruppen wird dazu verwendet, unterschiedliche Arten von Nachrichten zwischen dem CKS und dem CAS zu übertragen. Die zwei Gruppen sind der Steuersocket 380 und die Personalisierungssockets 370 bis 376.

Die Schnittstellen zwischen dem Chipkarten-Kontrollsystem CKS und dem externen Chipkarten-Administrationssystem CAS sind also Sockets in einer TCP/IP-Verbindung. Über diese Verbindung verlaufen die logischen Kommunikationskanäle zwischen den Chipkarten und dem Chipkarten-Administrationssystem

Neben den Personalisierungssockets wird also vom CKS ein weiterer Kommunikationskanal 360 für Personalisierungssteuernachrichten aufgebaut, und zwar unter Verwendung des Steuersockets. Unter Verwendung dieser Personalisierungssteuernachrichten wird der Personalisierungsvorgang durch eine Personalisierungsanforderungnachricht ausgelöst und die Erledigung wird mit einer Resultatnachricht bestätigt.

Nachdem die Chipkarte physikalisch kontaktiert wurde, wird durch das CKS ein Reset der Karte ausgelöst. Das CKS startet den Chipkarten-

Programmierungsvorgang, indem über den Steuersocket die Personalisierungsanforderungsnachricht an das CAS gesendet wird. Mit dieser Nachricht wird das CAS über den zu verwendenden Kommunikationskanal, bzw den Chipkarten-Personalisierungssocket, für die Personalisierungskommandos und Personalisierungsnachrichten informiert, ferner über das Kommunikationsprotokoll und andere Informationen über die Chipkarte (z. B. die Resetinformationen) und die Anforderung, die verarbeitet wird. Das CAS wiederum sendet die Personalisierungskommandos an den entsprechenden Chipkarten-Personalierungssocket unter Verwendung des korrekten Kommunikationsprotokolls. Gemäß dem vorgeschriebenen Kommunikationsprotokoll entpackt dann das CKS die Personalisierungskommandos und sendet sie an den Chipkarten-Koppler. Ein Teil der Personalisierungskommandos kann dabei dabei z. B. Steuerinformation sein, die einen Timeout anzeigt, der für die Ausführungsdauer des Personalisierungskommandos für die Chipkarte gilt. Die Personalisierungskommandos selbst werden transparent ohne Modifizierung auf die Chipkarte übertragen. Ausnahme bilden hier nur Kommandos, die vom CKS einen Reset des Chips anfordern. Die Antwortnachrichten der Chipkarte wiederum werden transparent über das CKS an das CAS unter Verwendung des gleichen Personalisierungssockets und desselben Kommunikationsprotokolls übertragen.

Unterschiedliche Arten von Nachrichten werden über unterschiedliche Socketgruppen ausgetauscht. Personalisierungsnachrichten, die Personalisierungskommandos von dem CAS repräsentieren, sowie die Chipkartenantworten auf diese Kommandos, werden über den Chipkarten-Personalisierungssocket ausgetauscht bzw. übertragen. Steuernachrichten während der Verarbeitung, etwa um den Chipkarten-Personalisierungsvorgang anzufordern, die Erledigung der Personalisierung zu berichten, oder um Statusnachrichten auszutauschen, werden unter Verwendung des Steuersockets übertragen. Abgesehen von den Resetanforderungen für eine Chipkarte, welche vom CAS an das CKS übertragen werden, werden die Personalisierungsnachrichten transparent zwischen der Chipkarte und dem CAS über das CKS übertragen. Während des Personalisierungsvorganges können auch Chipkarten-Resetanforderungen vom CAS über den Personalisierungssocket an das CKS geschickt werden. Der

Steuersocket wiederum wird verwendet, um Steuernachrichten zu und von dem Chipkarten-Administrationssystem zu übertragen. Für ein Chipkarten-Kontrollsystem gibt es genau einen Steuersocket. Die über diesen Socket übertragenen Steuernachrichten umfassen dabei beispielsweise:

- Anforderungen zur Durchführung einer Personalisierung
- Personalisierungs-Resultatnachrichten.

Die Personalisierungssockets werden dazu verwendet, Personalisierungsnachrichten zwischen dem CAS und dem CKS während des Programmierungsvorgangs des Chips zu übertragen. Ein Chipkarten-Koppler ist dabei logisch einem dieser Personalisierungssockets zugeordnet. Das Chipkarten-Kontrollsystem baut intern einen Kommunikationskanal zwischen dem Personalisierungssocket und dem entsprechenden Chipkarten-Koppler auf. Die Programmierkommandos (außer Resetanforderunngen) und Antwortnachrichten der Chipkarte werden transparent über den so entstehenden logischen Kommunikationskanal zwischen Chipkarte und Chipkarten-Administrationssystem übertragen. Das Chipkarten-Kontrollsystem muß diese lediglich gemäß dem Kommunikationsprotokoll entpacken bzw. korrekt weiterleiten, und zwar an den Chipkarten-Koppler, der dem Socket zugeordnet ist, von dem die Nachricht empfangen wurde. In umgekehrter Richtung muß das Chipkarten-Kontrollsystem die Antwortnachricht gemäß dem Anwendungs-Protokollformat "verpacken" bzw. formatieren und sie an das Chipkarten-Administrationssystem unter Verwendung des zugeordneten Personalisierungssockets abschicken.

Gibt es für die Chipkarte kein Resetkommando, muß ein Reset über das entsprechende elektrische Signal an den Chipkartenkontakten ausgelöst werden. Dieses Signal wird vom Chipkarten-Koppler erzeugt. Wird während des Personalisierungsablaufs ein Reset der Chipkarte benötigt, so wird dieser mit einem Resetkommando über den Personalisierungssocket an das CKS übertragen. Dieses Kommando muß vom CKS interpretiert werden und in ein entsprechendes Resetkommmando für den Chipkarten-Koppler umgewandelt werden. Die Chipkartenantwort auf den Reset (ATR, answer to reset) wird wiederum transparent an das CAS übertragen.

Nach Erledigung der Personalisierung der Chipkarte erzeugt das CAS eine Personalisierungs-Resultatnachricht und sendet diese ab. Diese Nachricht umfaßt das Programmierergebnis und eventuell einige weitere Informationen, z.B. Informationen, die für die weitere Verarbeitung der Chipkarte wichtig sind. Falls während des Personalisierungsvorgangs ein Fehler auftritt, wird die Chipkarte von dem CKS als fehlerhaft aussortiert.

Auch in vorliegendem Ausführungsbeispiel dient das Chipkarten-Kontrollsystem als Router, der die letztlich für die Chipkarte bestimmten Daten vom Chipkarten-Administrationssystem empfängt und transparent, d. h. unverändert, an die Chipkarte weiterleitet, für die die Daten bestimmt sind. Bei diesem Ausführungsbeispiel ist es jedoch möglich, mehrere Chipkarten bzw. die Personalisierung für mehrere Chipkarten gleichzeitig zu verarbeiten.

In einem weiteren Ausführungsbeispiel ist es denkbar, daß mehrere Chipkarten-Kontrollsysteme, gegebenenfalls über verschiedene Datenleitungen, mit einem Chipkarten-Administrationssystem verbunden sind, daß beispielsweise jedes dieser Chipkarten-Kontrollsysteme eine oder mehrere Chipkarten bearbeiten kann und daß die von den unterschiedlichen Chipkarten-Kontrollsystemen angeforderten Anwendungen unterschiedlich sind. Über eine am Chipkarten-Kontrollsystem vorgesehene Benutzerschnittstelle oder die Zuordnung von Produktionsaufträgen zu unterschiedlichen Auftragstypen kann das CKS unter mehreren möglichen Anwendungen, etwa einer Personalisierung, Initialisierung oder der Durchführung einer weiteren Chipkartenanwendung wie etwa einer Authentifizierung auswählen.

Für den Fachmann ergeben sich leicht weitere Modifikationen der vorliegenden Erfindung. Beispielsweise kann es sich bei den beschriebenen Chipkartenanwendungen neben einer Authentifizierung auch um andere Anwendungen handeln, bei denen ggf. ein interaktiver Informationsaustausch zwischen Chipkarten-Kontrollsystem und dem Karteninhaber vorgesehen sein kann.

Beispielsweise kann auch das Kontaktieren der Chipkarte drahtlos erfolgen. Anstelle eines mechanischen Kontaktes tritt dabei die Kontaktierung über hochfrequente elektromagnetische Wellen. Dabei erfolgt sowohl die Übermittlung der Daten als auch die Spannungsversorgung drahtlos. Beispielsweise wird mittels einer Induktivität auf der Chipkarte und ausgelöst durch ein Hochfrequenzsignal die Versorgungsspannung der Chipkarte erzeugt. Die weitere Kommunikation erfolgt mittels bekannter Hochfrequenztechniken.

Ansprüche

1. Verfahren zum Durchführen einer elektronischen Personalisierung und/oder Initialisierung einer Chipkarte und/oder einer Chipkartenanwendung, gekennzeichnet durch die folgenden Verfahrensschritte:

Kontaktieren der Chipkarte durch eine erste Vorrichtung;

Aufbauen oder Bereitstellen einer Verbindung zwischen der ersten Vorrichtung und einer separaten zweiten Vorrichtung zur Ausbildung eines logischen Kommunikationskanals zur Ermöglichung einer Kommunikation zwischen Chipkarte und der zweiten Vorrichtung über die erste Vorrichtung;

Anforderung der Durchführung einer Personalisierung und/oder Initialisierung der Chipkarte und/oder der Durchführung einer Chipkartenanwendung durch die zweite Vorrichtung von der ersten Vorrichtung; und

Durchführung der angeforderten Personalisierung und/oder Initialisierung der Chipkarte und/oder der angeforderten Chipkartenanwendung unter Verwendung der transparenten Übertragung von Daten und/oder Befehlen zwischen Chipkarte und zweiter Vorrichtung über den logischen Kommunikationskanal.

2. Verfahren nach Anspruch 1, bei dem

die Anforderung einer Anwendung Informationen über den zu verwendenden logischen Kommunikationskanal und die durchzuführende Anwendung enthält;

die zur Durchführung der angeforderten Personalisierung und/oder Initialisierung und/oder Chipkartenanwendung erforderliche Ablauflogik von der zweiten Vorrichtung ausgeführt wird; und

die zweite Vorrichtung das Ergebnis bezüglich der durchgeführten Ablauflogik an die erste Vorrichtung übermittelt.

3. Verfahren nach einem der beiden vorhergehenden Ansprüche, ferner gekennzeichnet dadurch, daß

die Anforderung der Durchführung einer Personalisierung und/oder Initialisierung und/oder der Durchführung einer Chipkartenanwendung Informationen bezüglich der Kommunikation, der zu verwendenden Kommunikationsadresse und des zu verwendenden Kommunikationsprotokolls enthält, sowie ferner Informationen über

die angeforderte Anwendung, die kontaktierte Chipkarte und eine Identifikation des angeforderten Vorgangs innerhalb der ersten Vorrichtung und daß

nach Durchführung der Personalisierung und/oder Initialisierung und/oder Chipkartenanwendung der logische Kommunikationskanal durch die erste Vorrichtung abgebaut wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß

die Ablauflogik oder Algorithmen für deren Durchführung sowie entsprechende Schlüssel in der zweiten Vorrichtung gespeichert sind.

5. Verfahren nach einem der vorhergehenden Ansprüche, bei dem

die von der zweiten Vorrichtung ausgeführte Ablauflogik eine Authentifizierung ist.

6. Vorrichtung zum Durchführen einer elektronischen Personalisierung und/oder Initialisierung einer Chipkarte und/oder zum Durchführen einer Chipkartenanwendung, welche aufweist:

eine Einrichtung zum Bereitstellen oder Aufbauen einer Verbindung mit einer weiteren Vorrichtung, die zum Kontaktieren einer Chipkarte dient, zur Ausbildung eines logischen Kommunikationskanals zur Ermöglichung der Kommunikation zwischen der Chipkarte und der Vorrichtung über die weitere Vorrichtung;

eine Einrichtung zur Aufnahme der Anforderung zur Durchführung einer Personalisierung und/oder Initialisierung und/oder Durchführung einer Chipkartenanwendung über die Verbindung;

eine Einrichtung zur Durchführung einer Ablauflogik für die angeforderte Personalisierung und/oder Initialisierung und/oder durchzuführende Chipkartenanwendung in Reaktion auf die Anforderung; und

eine Einrichtung zur transparenten Übertragung von die Durchführung betreffenden Daten und/oder Befehlen von und zu der Chipkarte über den logischen Kommunikationskanal.

7. Vorrichtung zur Durchführung einer elektronischen Personalisierung und/oder Initialisierung einer Chipkarte und/oder zur Durchführung einer Chipkartenanwendung, welche aufweist:

eine Einrichtung zum Kontaktieren einer Chipkarte;

eine Einrichtung zum Bereitstellen oder zum Aufbauen einer Verbindung mit einer weiteren Vorrichtung, in der die zur Durchführung der Personalisierung und/oder Initialisierung und/oder Durchführung der Chipkartenanwendung erforderliche Ablauflogik ausgeführt wird, zur Ausbildung eines logischen Kommunikationskanals zur Ermöglichung einer Kommunikation zwischen Chipkarte und der weiteren Vorrichtung über die Vorrichtung;

eine Einrichtung zum Anfordern der Durchführung der Personalisierung und/oder Initialisierung und/oder der Chipkartenanwendung durch die weitere Vorrichtung; und

eine Einrichtung zur transparenten Übertragung von die Durchführung betreffenden Daten und/oder Befehlen zwischen der weiteren Vorrichtung und der Chipkarte über den logischen Kommunikationskanal.

8. System zur Durchführung einer Personalisierung und/oder Initialisierung und/oder einer Chipkartenanwendung, welches umfaßt:

eine erste Vorrichtung zum Kontaktieren der Chipkarte;

eine separate zweite Vorrichtung zum Durchführen für die Personalisierung und/oder Initialisierung einer Chipkarte und/oder zur Durchführung einer

Chipkartenanwendung erforderlicher Ablauflogik in Reaktion auf eine Anforderung durch die erste Vorrichtung;

eine Einrichtung zum Bereitstellen oder Aufbauen einer Verbindung zwischen der ersten Vorrichtung und der zweiten Vorrichtung zur Ausbildung eines logischen Kommunikationskanals zur Ermöglichung der Kommunikation zwischen der Chipkarte und der zweiten Vorrichtung über die erste Vorrichtung; und

eine Einrichtung zur transparenten Übertragung von die Durchführung betreffenden Daten und/oder Befehlen zwischen der zweiten Vorrichtung und der Chipkarte über den logischen Kommunikationskanal.

9. System nach Anspruch 8, bei dem die erste Vorrichtung ferner umfaßt:

eine Einrichtung zum Kontaktieren mehrerer Chipkarten;

eine Einrichtung zur Ausbildung jeweils mindestens eines logischen Kommunikationskanals zwischen jeweils einer der Chipkarten und der zweiten Vorrichtung über die erste Vorrichtung; und

eine Einrichtung zum Absenden mehrerer Anforderungen zur Durchführung von Personalisierungen und/oder Initialisierungen und/oder Chipkartenanwendungen durch die zweite Vorrichtung.

10. System nach Anspruch 8 oder 9, bei dem die zweite Vorrichtung ferner umfaßt:

eine Einrichtung zum Bereitstellen oder Aufbauen mehrerer logischer Kommunikationskanäle; und

eine Einrichtung zum Durchführen mehrerer Personalisierungen und/oder Initialisierungen und/oder Chipkartenanwendungen in Reaktion auf Anforderungen von einer oder mehreren ersten Vorrichtungen.

11. System nach einem der Ansprüche 8 bis 10, das ferner umfaßt:

eine Einrichtung der ersten Vorrichtung zum Erzeugen eines oder mehrerer Server-Sockets;

eine Einrichtung der zweiten Vorrichtung zum Erzeugen eines oder mehrerer Client-Sockets; wobei

ein oder mehr Client-Server-Socketpaare zur Kommunikation zwischen Chipkarte und zweiter Vorrichtung verwendet werden.

12. System nach einem der Ansprüche 8 bis 11, bei dem ein Client-Server-Socketpaar zur Übertragung von Befehlen oder Daten betreffend die Personalisierung und/oder Initialisierung und/oder Chipkartenanwendung verwendet wird, und

ein Client-Server-Socketpaar zur Übertragung von Steuernachrichten verwendet wird.

13. System nach einem der Ansprüche 8 bis 12, bei dem die von der zweiten Vorrichtung durchgeführte Ablauflogik eine Authentifizierung oder eine andere sicherheitskritische Anwendung umfaßt.

14. System nach einem der Ansprüche 8 bis 13, bei dem die zweite Vorrichtung mindestens eines der folgenden Merkmale umfaßt:

eine Einrichtung zur Durchführung mindestens eines Teils der zur Durchführung einer sicherheitsrelevanten Anwendung erforderlichen Ablauflogik; und

die zur Durchführung einer sicherheitsrelevanten Anwendung erforderlichen Schlüssel.

15. System nach einem der Ansprüche 8 bis 14, bei dem

die zweite Vorrichtung mehrere Anforderungen gleichzeitig bearbeiten kann und

die erste und zweite Vorrichtung jeweils eine Einrichtung zum Ver- bzw. Entschlüsseln der zwischen ihnen übertragenen Daten umfassen.

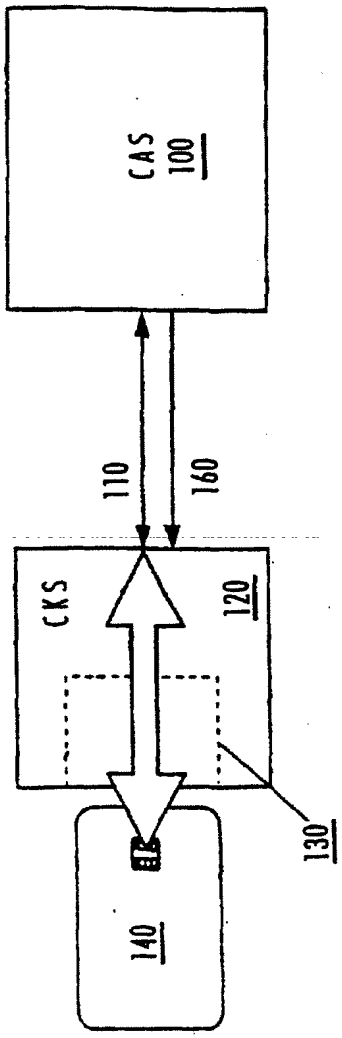


Fig. 1

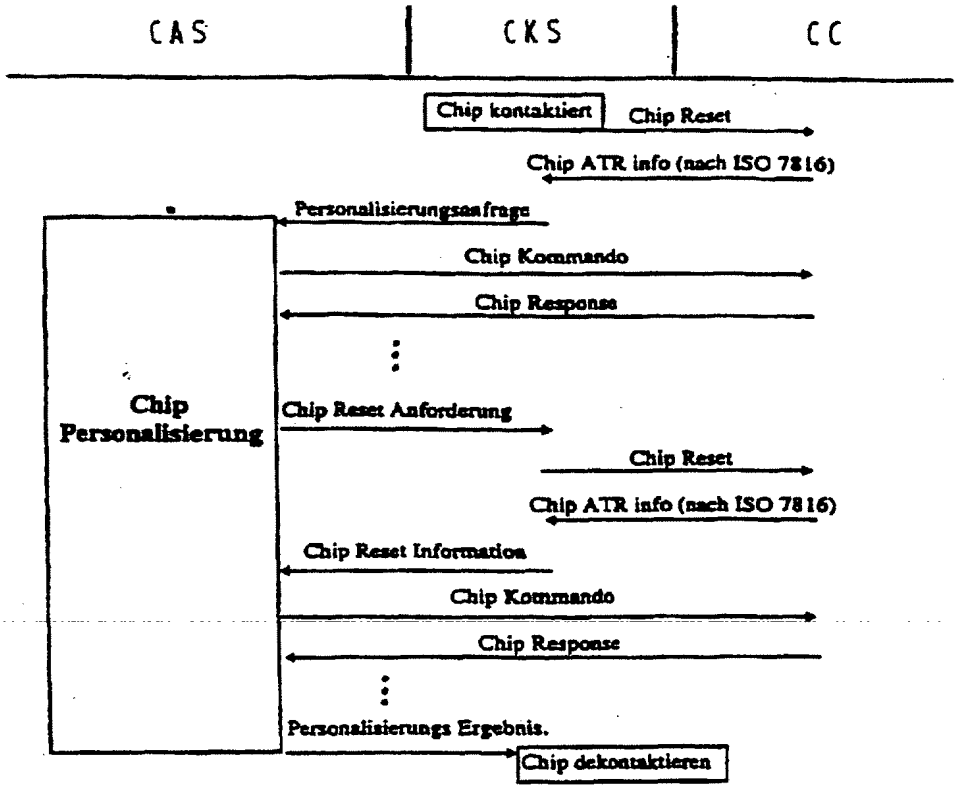

CAS
CKS
CC
Chip kontaktiert
Chip Reset
Chip ATR info (nach ISO 7816)
Personalisierungsanfrage
Chip Kommando
Chip Response
Chip Personalisierung
Chip Reset Anforderung
Chip Reset
Chip ATR info (nach ISO 7816)
Chip Reset Information
Chip Kommando
Chip Response
Personalisierungs Ergebnis.
Chip dekontaktieren

Fig. 2

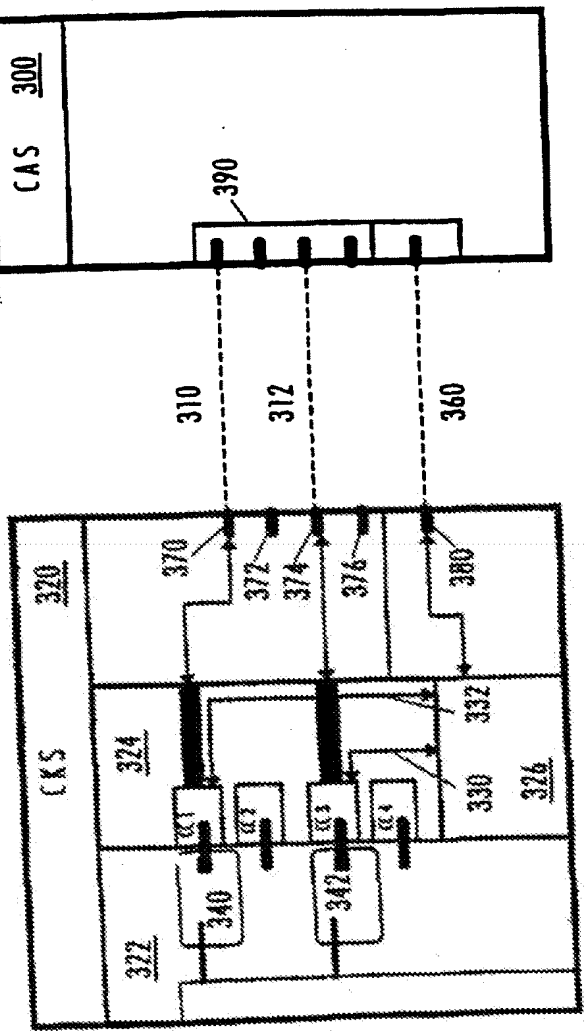

CAS 300
390
310
312
360
320
370
372
374
376
380
CKS
324
332
330
326
322
340
342

Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/01360

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06K17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 266 926 A (THORN EMI MALCO INC) 11 May 1988 see column 5, line 28 - line 33 see column 6, line 8 - line 12	1-3,5-8
A	EP 0 256 921 A (BONNEMOY MARC) 24 February 1988 see column 3, line 12 - line 22 see column 7, line 24 - line 30 see column 13, line 29 - line 34 see claims 3,4	1-3,6,8, 10,11
A	US 4 825 054 A (RUST JEFFREY J ET AL) 25 April 1989 see column 3-5 see claims 1,2,4	1-3,6-8

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 October 1998	02/11/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Herskovic, M

1

Form PCT/ISA/210 (second sheet) (July 1992)